Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

TO: NATO Allied Command Transformation (ACT)

FROM: Delharty Manson, *Forward* Defense Program, Atlantic Council

DATE: December 13, 2023

SUBJECT: Expanding NATO's competitive mindset: Deterring and defending across physical and virtual domains

---

In October 2023, the Scowcroft Center for Strategy and Security's Forward Defense program, in partnership with NATO ACT, convened current and former practitioners for a private workshop on expanding NATO's competitive mindset. Participants discussed NATO's approach to multi-domain operations (MDO) across physical and nonphysical domains, identifying key challenges and opportunities to operationalize MDO across the Alliance. This memo summarizes the workshop's key takeaways and conclusions and is informed by discussion papers written by Tate Nurkin, Margaret Smith, and Justin Lynch.

Strategic Context

While NATO's mission has historically focused on deterring aggression from Russia in the European theater, it today faces a security environment that is far more complex and global in nature. As Russia's war in Ukraine wages on, and China takes an increasingly assertive position on the global stage, NATO now faces a range of challenges including threats below the threshold of armed conflict and in nonphysical spaces. These emerging threats are intensified by innovative technologies from the commercial sector that bring scale and speed to battlefield effects. In response, the 2021 NATO Warfighting Capstone Concept (NWCC)—which acknowledges that the Alliance's "operating environment is widening beyond traditional military bounds"—proposes a proactive and anticipatory approach to rising security threats from Russia and China through multi-domain operations.[1] MDO requires that the Alliance update, expand, and align its approach to targeting and maneuver across all domains (air, land, sea, space, cyber, and information) and on a global scale to impose strategic costs on, and security dilemmas for, opponents.

The Modern Threat Environment and Implications for Targeting and Effects Generation

Nonphysical domains (cyber, space, and information)—which have long presented challenges to transatlantic security—are taking on a renewed importance as rapid advancements in commercial technology transform the speed and magnitude of military targeting and effects generation. China and Russia have invested in capabilities cutting across the space, cyber, and information domains, and are targeting and degrading the Alliance's unity and ability to fight before conflict even begins. This emerging security environment leads to several implications for NATO's targeting and effects generation.

- *A Battlespace Where Artificial Intelligence (AI) Systems Increasingly Create an Edge.* AI-enhanced systems will increasingly generate consequential effects on the battlefield, by enabling faster and more informed decision-making and enabling autonomous support. Machines can currently process and

[1] "NATO Warfighting Capstone Concept," NATO Allied Command Transformation, 2023, https://www.act.nato.int/wp-content/uploads/2023/06/NWCC-Glossy-18-MAY.pdf.

respond to information much faster than the human brain processes—let alone reacts to—information. NATO's adversaries are taking advantage of commercially available AI technologies to increase the scale and type of nonphysical attacks, including leveraging generative AI to support influence operations and cyberattacks. While the war in Ukraine has emphasized the critical importance of traditional hardware and ammunition, dual-use technological advancements have been leveraged on the battlefield and will likely increase the speed of battlefield responses in the future. With machines' speed advantage over humans, NATO's MDO doctrine will need to anticipate a future in which competition and conflict in all domains occur rapidly—and increasingly between systems rather than people—and field similarly advanced systems to maintain its technological edge.

- *The Civil Sector and Commercial Industry's Role in Conflict.* Today's battlespace is also enabled by a range of commercial and civil-sector technologies and capacities, and NATO must consider how non-military infrastructure fits into its MDO plans. For instance, transportation and information-technology (IT) infrastructure boosts warfighting capabilities but is vulnerable to attack because adversaries may see it as military infrastructure. Additionally, commercial companies lead in the development of cutting-edge dual-use technologies that have significant utility for defense, such as SpaceX's network of satellites used in Ukraine. Moreover, government-provided material support to Ukraine has been delivered via civilian airports, roads, and railway networks. However, as these commercial technologies and civil-support systems become ever more connected to the frontline of warfare, they will also be at greater risk of destruction by adversaries. As a result, a robust NATO MDO approach must consider not only how to leverage and integrate these civilian capacities, but how to defend them in the event of conflict.

- *Persistent Engagement Below the Threshold of Conflict*. Conflict does not begin with the first physical shot fired. Rather, competition is ongoing across all levers of national power where operations—particularly in the cyber and information domains—can destabilize NATO member states and chip away at their security without escalating to armed conflict. Tools employed in cyberspace help in this effort by planting malware, hacking critical systems, or using media platforms to discredit NATO member governments and advance an opponent's narrative. These activities can operate constantly without necessarily escalating to armed conflict, but still degrade NATO's cohesion and ability to defend itself during conflict. In turn, NATO must be prepared to engage adversaries in cyberspace and the information domain in order to counter attempts to undercut Alliance strengths prior to conflict.

- *Operating in a Global and Interconnected Threat Environment.* The NWCC acknowledges that NATO's security environment increasingly involves "competition among different actors becoming more persistent across all instruments of power," while identifying actors outside of Europe, notably China. This interconnected and global challenge to NATO is being actively demonstrated through the war in Ukraine, which is occurring within an international context. While Russia was initially isolated after invading Ukraine, China, Iran, and North Korea have since continued to support Russia by supplying it with weapons, oil, and security cooperation. This nascent block of authoritarian governments runs counter to NATO's interests beyond the European theater, including in the Middle East and the Indo-Pacific. In the interest of all its member states, NATO needs to prepare to outcompete and deter adversaries around the world and along a global contact layer, recognizing that no single conflict or

theater exists in a vacuum. Just as the war in Ukraine has involved states from multiple regions outside of the North Atlantic, so, too, will the security challenges that the Alliance faces in the future.

Challenges and Opportunities for Implementing Multi-Domain Operations

At both the national and Alliance levels, efforts to introduce and adopt multi-domain operations must address several challenges and capitalize on specific opportunities.

- *Definitions and Language*. Variations of multi-domain integration concepts exist across the NATO Alliance, with different member-state militaries having developed their own concepts—take, for example, the United States' combined joint all-domain command and control (CJADC2) concept. However, the development and progress made on these concepts vary. As a result, effective cross-Alliance multi-domain operations and integration should begin with an effort to more explicitly define and align key terminology and the scope of concepts associated with the multi-domain environment.

- *Data Access, Sharing, and Interoperability*. A key question for NATO in expanding its cyber operations is how its thirty-one member states can share critical data and intelligence despite different cultures and internal classification processes. NATO ought to focus on "synchronizing and, in some cases unifying, [its] approach to aggregating, storing, and analyzing data."[2] At the same time, the Alliance should embrace its diversity of membership when drawing conclusions from and using data. Understanding each member state's perspective on shared data ultimately enhances Alliance-wide decision-making. In addition to military data sharing, commercial data—like those from Starlink in Ukraine—have become increasingly important as an open source of unclassified information, which is easier to share and acquired differently than classified data. However, leveraging commercial data for defense operations requires continual access to data (which is not assured with private companies, as the war in Ukraine has also shown) and the ability to share information across NATO member states (which could create data-ownership issues). Increased data sharing in the Alliance will also be critical for training and supporting AI-enhanced systems that can be leveraged to boost information awareness, data collection, and decision support.

- *Lack of Political Appetite among NATO Allies to Engage in the Cyber Domain*. Despite the prevailing view of NATO as a purely defensive (and, in effect, reactive) Alliance, NATO's persistent engagement is necessary to effectively compete with its adversaries. Still, NATO members may view activities related to persistent engagement as persistent campaigning. Persistent engagement refers to using the cyber and information domains to deter and defend against aggression. On the other hand, persistent campaigning involves actions in both nonphysical and physical domains that demonstrate capability in order to deter aggression, such as military exercises. However, persistent campaigning can also be viewed—including by some NATO members—as an escalation toward conflict. NATO military planners should stress the difference between the two, as persistent engagement would not realign NATO's mission as a defensive alliance, but rather set a goal to proactively counter malign activity below the threshold of armed conflict in the cyber and information domains, in order to ensure that

[2] Maggie Miller and John Sakellariadis, "Russian Cybercrime Gang Hacks Federal Agencies," Politico, June 15, 2023, https://www.politico.com/news/2023/06/15/multiple-federal-agencies-hit-by-hack-00102229.

NATO's battlefield advantages remain. While NATO has long operated in the cyber domain, NATO requires a common language to employ cyber tools more effectively, norms to generate a shared understanding of offensive options across member states, and a collective strategy to compete in the cyber domain. This will allow more hesitant members the room to compete at their own pace, while allowing NATO not to be outpaced by adversaries.

- *Expanding NATO Maneuver across a Global Contact Layer.* One of NATO's greatest challenges is the allocation of scarce military resources in a multilateral Alliance with many competing interests within the European theater and across the globe. In addition, NATO members increasingly face deep internal divisions at the state level that have resulted in divided governments that typically find it difficult to agree on funding basic government needs, let alone agreement with other NATO members. NATO should develop a centralized, data-centric risk-management process to balance competing interests and align resources with a global strategy that prioritizes deterrence. A data-centric approach can provide a standardized metric for how the Alliance can view current and emerging crises and their urgency for a response across the globe. From that unified viewpoint, prioritizing resources to deter multiple adversaries simultaneously—while still a difficult process—should focus on placement and access (virtual and physical) to an entity of interest; situational awareness of an entity (actor and/or location) in broader geostrategic planning; and ability to develop effective and efficient options to respond.[3] One method for prioritizing the allocation of resources would be to develop operational plans for data and information collection and analysis to inform enhanced decision-making. Each operational plan would require detailed force requirements of personnel, intelligence-collection assets, basing, and other resources.

- *Recruitment Competition with the Commercial Sector*. Human capital is key to maintaining NATO's strategic advantages in achieving diversity, resilience, and sufficient mass to conduct operations. However, recruiting and retaining military personnel is increasingly challenging, especially as NATO populations are declining and aging. To further complicate matters, the same qualities that are highly sought after by NATO in personnel—broad minded, intellectually agile, technically proficient, and collaborative—are also sought by the commercial sector. NATO and its members should consider how it can compete in recruitment with attractive private employers. In some cases, NATO may need to partner with other institutions, such as universities that lead the way in researching the technologies and strategies critical to NATO's defense. In addition, NATO must be able to articulate the type of personnel it needs, just as it does for military technology. Attracting and training qualified personnel is just as essential to data collection and MDO as AI-enhanced intelligence-collection and analysis systems.

- *Adversary Innovation and Adaptation*. Russia, China, and other NATO adversaries will not stand idly by as NATO adopts and employs new technologies and strategies. Russia is adapting militarily based

[3] Gen James E. Cartwright, et. al., *Operationalizing Integrated Deterrence: Applying Joint Force Targeting across the Competition Continuum,* Atlantic Council, June 8, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/operationalizing-integrated-deterrence-evolving-the-joint-forces-application-of-targeting-across-the-competition/.

on lessons learned from its war in Ukraine. Instead of rushing in ground forces, as it did with little success at the start of the war, Russia has instead used drones and other precise munitions to strike Ukrainian targets, essentially mimicking Ukraine's approach to attacking Russian troops since the start of the invasion. As in Ukraine, NATO's adversaries will continue to adopt innovative techniques to challenge the Alliance and the broader global order. In response, NATO must continually analyze the state of the battlespace and the capabilities of NATO adversaries, while working with the commercial sector to out-innovate adversaries and maintain the Alliance's technological edge.

Concluding Thoughts and Areas for Further Discussion

NATO's ability to accomplish its mission to deter and, if necessary, defend against aggression will continue to be challenged by persistent geopolitical and technological threats, both conventional and in the gray zone. To meet these challenges and maintain NATO's enduring military advantage and deterrence strategy, the Alliance should strengthen its ability to implement and integrate MDO. MDO allows allies to operate simultaneously in and across physical and nonphysical domains, which offers opportunities to disrupt adversaries' decision-making, command and control, and freedom of action. However, MDO can only be successful if NATO sets a desired end state and conceptualizes what victory looks like across the competition continuum. Competition is both a state and a process; NATO can expand its competitive mindset to continually evolve its strategies and tactics in anticipation of, and response to, adversarial behavior.